File Backup Guidance

Guidance Sections

SECTION 1
Orientation and Advice

Introduction

When a computer security incident or other unforeseen event occurs that results in a loss of data, recovery from the incident or event requires up-to-date backups and proven methods of restoring the data. This document contains guidance on the categorization, frequency, type, handling (e.g. log books, labeling), storage, and retention of backups for both critical and non-critical systems at NIH. The intended audience includes managers and LAN and System Administrators. The guidance includes backup advice, the backup services, and procedures currently in place at NIH, and links to web sites with backup information.

Background

Some organizations make daily backups, but never verify that the backups are actually working. Others construct backup policies and procedures, but do not create restoration policies and procedures. Such errors are often discovered when a hard disk fails, data is corrupted, or after a hacker has entered systems and destroyed or otherwise compromised data.

A second problem involving backups is insufficient physical protection of the backup medium. The backups contain the same sensitive information that reside on the computer and should be protected in the same manner.

Backups aid in recovering your system in the event of loss of data due to:

- Security Incidents
- Denial of Service (DoS) attacks
- Accidents or other deletion
- System failures
- Disasters.

Backups and associated procedures are critical in times of emergency, support security recovery efforts, and aid in IT security forensics investigations, and FBI investigations.

For mission critical applications, backup procedures must be formally documented and part of the System Security Plan (SSP). Formal documentation comes in the form of: Contingency Plans, Disaster Recovery Plans (DRPs), and Business Contingency and Continuity Plans (BCCPs). IT Security Risk Assessments and federally mandated IT security audits verify these contingency documents and review the verification/certification tests. However, the ultimate responsibility lies with the system administrator and system manager to implement and test these procedures.

Types of Backups

There are basically three types of backups:

1. Full. Full backups include the operating system, special programs, COTS packages, scripts, and data files. Full backups cover all the data on the system, database, or file, regardless of how much has been backed up during the most recent backup.

2. Incremental. Incremental backups contain a copy of only files that have changed since the previous backup. Be aware the there are two types of incremental backups (since the last full backup, and since the last incremental) and they vary by length and affect the backup and restore times.

3. Special/Custom. Special or custom backups are usually created for special circumstances like system reconfigurations and special applications.

Backup Guidelines

Backups for mission critical applications must be made at least daily. The minimum requirement guideline is to perform full backups weekly and incremental backups daily. At least once a month the backup media should be verified by doing a restore for selected files to a test server to verify that the data is actually backed up accurately, not corrupt, and can be restored.

File Backup Guidance

The following rules describe how to develop a complete, recoverable, and organized backup environment:

1. Establish backup frequency commensurate with the risk and criticality of the data.
2. Create backups on a regular schedule.
3. Establish, maintain, and review logs of backups.
4. Make sure special files (e.g. hardware drivers) are backed up.
5. Use relative pathnames for backups. E.g. for UNIX relative pathnames begin with a ./ or a directory name as opposed to /. It sets the path based on the current directory as opposed to the absolute pathname that must align itself only to the root. For Windows applications full pathnames should be avoided because the information would provide an intruder the exact location of the application, control files, and/or data.
6. Maintain physical security of the backup tapes.
7. Rotate the backup tapes/media (i.e. Don't use the same media every day).
8. Have a boot diskette in case of an emergency.
9. Have a copy of the restore utility on the bootable media (diskette or CD).
10. Backup file systems separately (e.g. / and /u on UNIX systems). Use separate disk drives if possible and have on a removable media.
11. Ensure data can be easily restored when necessary by verifying the backup data (i.e. periodically restore to a test machine, or verify with appropriate software scanning/testing tool).
12. Keep backup logs of file information (i.e. file list with date of each and label of tape) and backup errors, if any. Also record/track what was done in response to errors.
13. Label the backup tapes with date of backup, backup level, file systems backed up, sensitivity level, and any other pertinent information.
14. For mission critical applications keep off-site copies in a secure location. Not only mission critical applications but a copy of all backups should be kept off-site.
15. Backups should be encrypted whenever possible.
16. Replace backup media on a regular basis (at least yearly)
17. Ensure that up-to-date Antivirus software is running and that all files backed up are virus free.

Areas of Concern

There are four areas of concern:

1. Mission Critical Systems. In general, mission critical systems at NIH are described as ones where their loss or compromise could:
   - Potentially place human or animal life at risk, or
   - Adversely affect primary patient, animal, or scientific research data, or
   - Jeopardize a ubiquitous system that is central to the NIH mission or integral to the agency's infrastructure.

   The following backup guidelines apply to mission critical systems:
   - Make daily backups.

- When storing backup tapes off-site make certain the site is geographically removed from primary site.
- When storing tapes on-site put them in a locked fire and waterproof container.
- Store backup media in an environmentally safe and locked location/room.
- Verify the media regularly by doing validation tests and restoring media to test sites.
- Encrypt the data on the backup media if it contains sensitive data.
- Perform background checks on personnel that will be handling backup media for highly sensitive or mission critical systems. Background checks are required by regulation for all IT staff whether Government or Contractor.

2. <u>Servers</u> (web, file, printer, e-mail, etc.).

   The following guidelines will ensure an environment that is quickly recoverable:
   - Perform a full backup every time a new installation of the operating system or new application occurs. The backup must occur after configuration modifications have been completed, patches have been applied, and the system is functional. Also, consider making backups in a step fashion if the installation is long and complicated so reduce the effort in re-work should problems arise.
   - Save several generations of backup so that you can go back to a previous installation if problems occur.
   - Full data backups should occur at least weekly. Save at least the previous 3 weekly full backups before reusing the media.
   - At least 3 monthly full backups should be saved before reusing the media. (This will enable you to be able to restore back if you should find problems with restoring more current backups.)
   - Incremental data backups should be conducted daily.
   - Each day should be backed up on a different media.
   - Server log files should be stored on another machine.
   - Encryption should be considered when backing up sensitive data.
   - Backup media should be stored in a secure location in a fireproof and waterproof media container.
   - Previous weekly and monthly backup media should be stored in a geographically separated offsite location whenever possible.
   - Ensure that data backups are synchronized for database systems (which have multiple files) and for systems that span multiple platforms.

3. <u>User workstations</u>.

   The following guidelines are recommended for user workstations:
   - Backups of COTS software consist of the installation diskette or CD-ROM. Copies of the COTS (including operating systems) software should be kept in a fireproof and waterproof container (preferably off-site), making the need to back up software unnecessary. Users should be encouraged to put data they need on a file server which would be backed-up as described above.
   - It is the user’s responsibility to backup data stored on the hard drive.

- Users should on a regular basis copy data stored on a hard drive to the network so that it can be backed up.
- If data resides on a diskette and was used on a machine outside of NIH, use anti-virus software to scan the disk prior to using it to prevent accidental infection of the workstation.
- For Windows 2000 or Windows XP, backup data software is available under Start/Programs/Accessories/System Tools/Backup/Backup Wizard. Whenever possible, this backup should be made to either removable media or another system or the network.
- Anti-virus software should be kept up-to-date.
- Anti-virus software should be configured to automatically scan media before loading.

4. <u>Laptops</u>.

   Laptops are more portable than desktops and because they are more likely to be stolen, lost, or damaged the following guidelines apply in addition to the user workstation precautions:
   - Sensitive/critical data files should not be kept on the hard drive but on removable media that is regularly copied to a file server for backup.
   - COTS and operating system software should follow the same guidelines as mentioned in the user workstation section.
   - Data should be stored encrypted.
   - Never keep the only copy of sensitive data or information on a laptop.
   - Users are responsible for making backups of their data.
   - Diskettes used to store/move files should be scanned for viruses prior to use.
   - Prior to connecting to any NIH network you should scan the machine for viruses to verify that the laptop has not been infected.

Backup advice for UNIX machines can be found at:

- Making Backups and Restoring (UNIX) – Provides descriptions and examples of the basic utilities as well as specific backup utilities, tips, and quirks for HP, SGI, Solaris, and Linux.
  http://www.uwsg.indiana.edu/usail/backups/backup/

- Performing Backups and Restoring Files (UNIX - GNU tar) – This site focuses primarily on developing scripts and the 'Tar' and 'Dump' utilities.
  http://sunland.gsfc.nasa.gov/info/tar/Backups.html

Backup Schedules and Retention

Before deciding on a schedule for making backups a variety of considerations must be taken into account:

- Type of backup – Full, incremental, or special/custom.

File Backup Guidance

- Sensitivity level – Low, Moderate, or High. More information about the sensitivity levels can be found at - http://irm.cit.nih.gov/policy/DHHS_SecLev.html.
- Criticality of the system - Low, Moderate, or High. More information about the criticality levels can be found at - http://irm.cit.nih.gov/policy/DHHS_SecLev.html.
- User requirements – E.g. send to off-site storage.
- Timing of the backups – End of day, end of week, end of month, quarterly, etc.
- Storage media and hardware to be used – E.g. Zip drive, CD-ROM, diskette, etc.
- When to send backups off-site
- Daily responsibilities and work schedule
- Automatic runtime (batch) scripts – Decide and develop scripts that will simplify the backup process.
- Physical labeling. Backups with sensitive data must have labels that indicate special handling.
- Storage location – Fireproof and waterproof media containers recommended.
- Tape/media log books – Contains a record of what was backed up, when backups were taken, by whom, and the type of backup.
- Location of system audit log files. It is recommended that logs be contained on machines other than the one the system is located on if possible. Additionally configuring multiple machines to have one common file would simplify review of the logs.
- Reference documentation/procedures for all shifts
- Quantity of backups required (How many used and unused on hand?)
- Re-use of media (i.e. planned obsolescence)
- Whether the data should be encrypted - Files may already be encrypted as part of the application's requirements, or they can be encrypted before making backups.

The advisory web sites that follow and the other sections of this document can help you decide the appropriate backup and retention schedules:

- Backup Rotations – A Final Defense. This is a white paper that describes backup file rotations.
  http://www.sans.org/infosecFAQ/sysadmin/rotations.htm

- Electronic Data Retention Policy. This is a white paper about establishing an electronic data retention policy.
  http://www.sans.org/infosecFAQ/backup/retention.htm

- Backup Strategy: Ten Tapes Rotation - This article provides an explanation of how a ten-tape cycle works.
  http://www.acs.unimelb.edu.au/backups/strategy.html

- The Hows and Whens of Tape Backups – This article provides advice on making tape backups, and reviews various software backup utilities.
  http://www.networkcomputing.com/1205/1205ws1.html

- Creating a Backup Schedule – This is an article with questions and answers about creating a backup schedule.
  http://uwsg.indiana.edu/usail/backups/schedule/

- Encrypting Backups for Additional Security – This is an article about encrypting file backups. Some software packages are discussed.
  http://searchstorage.techtarget.com/tip/1,289483,sid5_gci756807,00.html

Media Storage:

Backups can be made on a variety of media: tapes, CD-ROM, diskettes, cassettes, Zip drives, etc., but whatever the media it is recommended that they be stored in a waterproof and fireproof container in secure location or locked room. A well-protected environment is essential for mission critical tapes and systems that require many backup media (i.e. an off-site tape library). If secure containers are not available, the backup media should be kept in a locked room. Critical files must be easily identifiable and housed in something that can easily be carried in the event of a fire. Fire drills should reinforce this practice. Also, individuals who have access to mission critical or highly sensitive backup tapes must have their backgrounds checked. (Background checks are required by regulation for all IT staff whether Government or Contractor). Backup media that is no longer used should either have the media sanitized or destroyed.

Information on backup packages, storage media, and media life expectancy can be found at the following web sites:

- Backup Packages – This article provides a brief description of four backup packages: ArcServe, OmniBack, Reliaty Backup, and Networker.
  http://www.uwsg.indiana.edu/usail/backups/packages/

- Choices in Backup Devices and Media – This paper reviews the limitations of floppy disks, magneto optical and floptical disks, optical disks, hard drives and disks, magnetic tapes, jukeboxes, and stack loaders.
  http://www.uwsg.indiana.edu/usail/backups/media/

- Storing Backups and Media Life Expectancy – This article discusses the life expectancies of: magnetic tapes (1 year), video tape (1-2 years), magnetic disks (5-10 years), optical disks (30 years), and write-once CDs (30+ years).
  http://www.uwsg.indiana.edu/usail/backups/storing/

Testing, Data Recovery, and Certification

Going through the motions of making backups without knowing if they are usable is an exercise in futility. To prevent this from happening, the backup media must be periodically tested to ensure its usability:

- For servers it is recommended that backup tapes be recovered on test servers. Regular testing is recommended. It is not uncommon to find that the backup media is not current or empty because (1) the hardware or software wasn't functioning properly, (2) the hardware mechanism hasn't been cleaned regularly, (3) the storage media has been re-used too many times, or (4) the storage media has outlived its life expectancy.

- For other environments (such as mainframe), the off-site location should be used. Software that scans/reads tapes can alternatively be used when available for both server and mainframe tapes, if available.

- For mission critical systems, the tapes and off-site backup equipment must be fully tested at least annually and in accordance with the testing of Contingency and Disaster Recovery Plans. Certification letters/forms that verify recovery tests are required documents for mission critical systems and must be saved for annual federal reviews.

Recommendations

Now that you know all about the concerns, proper procedures, and types of backups you should revisit you existing procedures to ensure that should you encounter a problem (e.g. lost or corrupted data) you can continue to work after a hopefully minor interruption. Make sure that someone is making backups, you have sufficient backup media, and have planned for their replacement when the time comes. **Readers should contact their ICs IT department for specific guidance.**

Section 2 provides information about CIT services that ICs should consider when developing contingency and disaster recovery plans. Additional advisory information can be found in the web site links contained in section 3.

SECTION 2
NIH Backup Facilities and Procedures

NIH Media Sanitization and Destruction

Diskettes and other magnetic storage media that contain any government data or software must be sanitized when they are no longer needed. Portable media may be reused after overwriting or degaussing, or they should be destroyed. Simply deleting a file is not sufficient to prevent someone from un-deleting the file later. Similarly formatting a hard drive is not sufficient to prevent someone from un-formatting the drive at a later time. NIH policy is to destroy backups when they are no longer needed.

The NIH sanitization policy web site is http://irm.cit.nih.gov/security/sanitization.html and associated guidance can be found at http://irm.cit.nih.gov/security/sanit_info.html.

NIH Backup and Recovery Service (NBARS)

File Backup Guidance

The NIH **B**ackup **A**nd **R**ecovery **S**ervice (NBARS), provided by CIT, allows owners of NIH file servers and personal computers connected to NIHnet to easily backup their critical data to a centrally maintained, secure repository. Automatic backups can be scheduled on a daily, weekly or monthly basis, or on-demand backups can be initiated by the owner of the file server or workstation at any time with a point and click user interface. Although NBARS is fully functional for backup/recovery of desktop data, CIT strongly encourages the use of file servers as the most efficient manner for storing and managing distributed data. **A**DSTAR **D**istributed **S**torage **M**anager (ADSM), a client/server product from Tivoli Systems, Inc., an IBM company, is used to implement the Backup and Recovery Service.

For more information on how ADSM works and how to begin using the service, consult the NBARS web site (http://silk.nih.gov/silk/nbars/).

NIH Computer Center Backup Procedures

For mainframe systems managed by the NIH Computer Center, see the following documents:

- NIH Computer Center User's Guide, Storage and Backup of Data.
- NIH Computer Center Disaster Recovery Plan, Backup and Off-Site Storage Procedures.

CIT's Advanced Laboratory Workstation (ALW) System Support

CIT provides backup and recovery support for UNIX systems to ICs via the ALW. ICs that subscribe to this service can obtain support in the areas of procurement, installation, configuration, backup, recovery, and remediation.

ALW makes backups of user home volumes and user data volumes each working day, Monday through Saturday, excluding Federal holidays. The daily backup takes a snapshot of user data as it was at approximately 6 A.M. of the same day. ALW can recover data depending on the age of the lost data.

To find out more about this service go to http://www.alw.nih.gov/About_ALW/Business_policy.html.

NIH Off-Site Storage Services

CIT has contracted with the First Federal Corporation to provide secure off-site storage services. The First Federal facilities and procedures meet Department of Defense standards for secure storage. The following services are provided under the contract CIT has with First Federal:

- Delivery of the backup tapes between the First Federal storage facility and the Computer Center on a bi-weekly schedule;
- Delivery of backup tapes (both those stored at the First Federal facility and at the NIH campus) to the hot site upon request and as directed by the Center (both for disaster recovery tests and for an actual disaster); and
- Delivery of the backup tapes from the hot site back to NIH.

File Backup Guidance

In general, First Federal can respond within two hours notice, twenty-four hours per day, three hundred sixty-five days per year. Data Vault Corporation in Herndon, VA is another company that can provide off-site storage. For more information on these and other companies that provide off-site storage services, contact your Procurement Officer.

NIH E-mail Backup Policy (http://irm.cit.nih.gov/policy/email_backup.html)

The use of electronic mail (E-mail) messages has become an integral part of conducting business at NIH. All E-mail messages, including those accessible from backup media, are subject to Freedom of Information Act (FOIA) requests, requests from congressional committees and subcommittees, discovery requests in litigation and official investigations. All E-mail messages are considered to be Federal records when they meet the criteria specified in the statutory definition; i.e.,

- they are made or received under Federal law or the conduct of agency business, and
- they are preserved or are appropriate for preservation as evidence of the agency's organization, functions, policies, decisions, procedures, operations or other activities, or
- contain information of value.

NIH's policy, in accordance with the recommendation of the National Archives and Records Administration, is that all E-mail messages that meet the definition of Federal records should be copied with the transmission data to a record keeping system--either hard copy or electronic--and then deleted from the E-mail system.

Because there are many different E-mail systems in use at NIH, the procedures for storing, backing up and restoring E-mail messages will vary from system to system. Additionally, each individual sending or receiving E-mail has the ability to retain individual E-mail messages for whatever period of time desired. The wide range of retention of E-mail messages can significantly complicate the search for E-mail records as part of a FOIA request or investigation. In the interest of minimizing the costs associated with storing and searching E-mail messages, the following policy is established:

- E-mail system administrators will retain general backup files for E-mail messages or disaster recovery files for the E-mail system for no more than 3 months. (Backup files and disaster recovery files are electronic files created to restore computer system files that have become inaccessible on a computer system.)

- E-mail system administrators will create or retain archive files of E-mail messages that do not meet the definition of a Federal record, only with the approval of the ICD records management officer. (An archive file is an electronic file created to store computer system files that have been removed (deleted) from a computer system.)

- Users of desktop systems and workstations should not make backup, disaster recovery or archive files of non-record E-mail messages.

SECTION 3
Other Helpful Backup Guidance/Information Sites

NIH:

- MVS System Disaster Recovery – October 2002 Disaster Plan for the CIT Data Center.
  http://datacenter.cit.nih.gov/pdf/disasterplan.pdf

Non-NIH:

- 11 Common Backup Mistakes and How to Avoid Them – This article describes backup mistakes and avoidance advice for UNIX machines.
  http://www.elinux.com/articles/bru.jsp

- Centralized Backups – This is a SANS white paper that describes a centralized backup strategy for corporations. Additional helpful links about backups are contained at the end of the document.
  http://www.sans.org/infosecFAQ/recovery/central.htm

- Security Considerations for Enterprise Level Backups – This is a SANS white paper about making backups from an enterprise perspective.
  http://www.sans.org/infosecFAQ/backup/enterprise_level.htm

- Disaster Recovery Planning with a Focus on Data Backup/Recovery – This SANS white paper reviews strategies for backups when planning for disasters.
  http://www.sans.org/infosecFAQ/incident/recovery.htm

- Configure Computers for File Backups – CERT developed this advisory on configuring and deploying workstations and servers.
  http://www.cert.org/security-improvement/practices/p032.html